Claims:

1. A system comprising a trusted computing platform and one or more logically protected computing environments, each of which is associated with at least one service or process supported by said system, the system being arranged to load onto said trusted computing platform data defining a predetermined security policy defining security attributes to be applied to one or more of the at least one service or process when said service or process is started.

2. A system according to claim 1 wherein the policy included one or more security rules for controlling operation of logically protected computing environments.

3. A system according to claim 2 wherein the or each security rule for at least one of the logically protected environments will include an execution control rule which defines the security attributes.

4. A system according to claim 3, wherein said security attributes include or comprise one or more capabilities to be provided to the respective logically protected computing environment when said service or process is started.

5. A system according to claim 3, wherein said security attributes include or comprise one or more functions which change or modify the capabilities of the respective logically protected computing environment when said service or process is started.

6. A system according to claim 3, wherein when a service or process is started said security attribute operate to cause the service or process to be placed and run in a specified logically protected computing environment.

7. A system according to claim 3, wherein said security attributes operate to modify a user id, a group id or a logically protected computing environment in which a service or process is to be run.

8. A system according to claim 3, wherein said security attributes operate to define a directory to which the service or process is to be chrooted.

9. A system according to claim 5, wherein said execution control rule can raise or lower a specified capability.

10. A system according to claim 5 or claim 9, wherein the security attributes operate to filter a set of capabilities of a logically protected computing environment and modifying only one or more of said capabilities as selected by said filtering means.

11. A system according to any one of the preceding claims, wherein said execution control rule specifies the service or process to which it applies by identifying the associated logically protected computing environment, with the effect that said rule applies only to services or processes specifying that logically protected computing environment.

12. A system according to any one of the preceding claims, wherein the files making up a service or process to which said execution control rule applies are of read-only configuration.

13. A system according to any one of the preceding claims, including means for monitoring operations performed by the system which modify names of files making up services or programs to which said execution control rule applies.

14. A system substantially as herein described with reference to the accompanying drawings.

15. A method of applying a security policy in a system including a trusted computing platform and one or more logically protected computing environments, each of which is associated with at least one service or process supported by said system, the method including the steps of starting a service or process associated with at least one of the logically protected computing environments; and controlling the operation of the at least one logically protected environment by applying, upon starting of the service or process, security attributes to the service or process.

16. A method according to claim 15 wherein the attributes are defined by execution control rules, which are included in security rules implementing at least part of the policy.

17. A method of applying a security policy in a system including a trusted computing platform, the method being substantially as herein described with reference to the accompanying drawings.